International Journal of Advancement in Engineering Technology, Management & Applied Science

Volume 3, Issue 6 June 2016 ISSN No: 2349-3224

Secured and Reduced Data and Bandwidth Satellite Image Communication

Naveen[1], Dr. Mohamed Rafi[2]

Research Scholar[1], Professor and Chairman[2]

Dept. of CS&E, UBDTCE, Davangere, India

Abstract: **In this paper, a new simple and fast method for image encryption and compression is proposed. It uses 10 bits key to secure the image. At the sender side first operation is encryption then compression. The decryption procedure is similar to that of the encryption but in the reverse order. In this paper it has been e implemented and tested the proposed method for sample images. Proposed method is compared with the existing methods using a standard technique of measuring the standard deviation, entropy, quality of encryption, histogram and visual method. It is found that the proposed method is showing the better result than that of the existing methods.**

Keywords: Cryptosystem; Encryption; Decryption; Compression; Decompression;

I. INTRODUCTION

Information can be exchanged in several ways between two communicating parties. There are four main ways of communication; text, audio, video, and image. In most of the communication like military, medical, etc. image makes more prominence. These applications might be sensitive in nature. The data while transmission in these applications might face problems. Those are like copying, distribution of copied data[1], or eavesdropping etc. In this context the user should take care about the security and confidentiality of the data to protect from the hackers. This process of making the data secure is called as encryption[2]. In this work we have taken the communication media as Image. The image is encrypted and sent to the receiving side. At the receiving end, this image is retrieved back to its original form. This is called decryption [3].

File size is one of the factors which decides the transmission time. If the size of the file to be transmitted is less, it needs less time to transmit. For reducing the file size, the method of compression is used[4].

Satellite communication is one of the areas which rely on information exchange[5]. Data collected by the satellite might be sensitive. Attackers continuously assess these data. So, it should be made available to only those who have the rights. This can be achieved by proper encryption[6]. In addition to security, bandwidth available for data transmission might be less. In this case, data size should be reduced. This can be done by using compression. So, the combination of encryption and compression helps in achieving these goals[7].

The rest of the paper is described as follows. Section 2 reviews some required basic primitives including related work. Section 3 gives our proposed method. Performance evaluation and security analysis of the proposed system are presented in Section 4. Finally, some conclusions are given in Section 5.

II. RELATED WORK

1. *Modular Additive Encryption*

In modular additive type encryption, logical operation used for encryption is '+'. That is, secret key will be modularly added to the pixels or to the individual color values to create encrypted image. During decryption, secret key will be subtracted from the encrypted image which produces original image. Since the color values ranges from 0 0 to 255, mod value of 256 is generally preferred for image encryption.

2. *Modular Multiplicative Encryption*

In modular multiplicative encryption, secrete key is modularly multiplied with the pixel values or individual color values of the input image. During decryption inverse of the secret key is multiplied with the pixel values of the encrypted image to restore the original image. Secret key must be a prime number. This is because, it is not possible to find the inverse of an even key value. The condition is that, gcd of the mod value and the key should be equal to one, which is not true for even key values.

3. *Public Key Cryptosystem*

In Public key cryptosystem, two keys are used. One key for encryption and another for decryption. This scheme is also known as asymmetric key cipher system[8].

4. Private Key Cryptosystem

In this cryptosystem, same key is used for both encryption. Hence, this system is also known as symmetric key cryptosystem[8].

5. Sieving Process

Sieving as the name indicates, is the process of filtering the combined RGB components into individual R, G and B components. Pixel is a 32 bit value made up of four components: alpha, red, green, and blue each of 8bits length.

III. PROPOSED METHOD

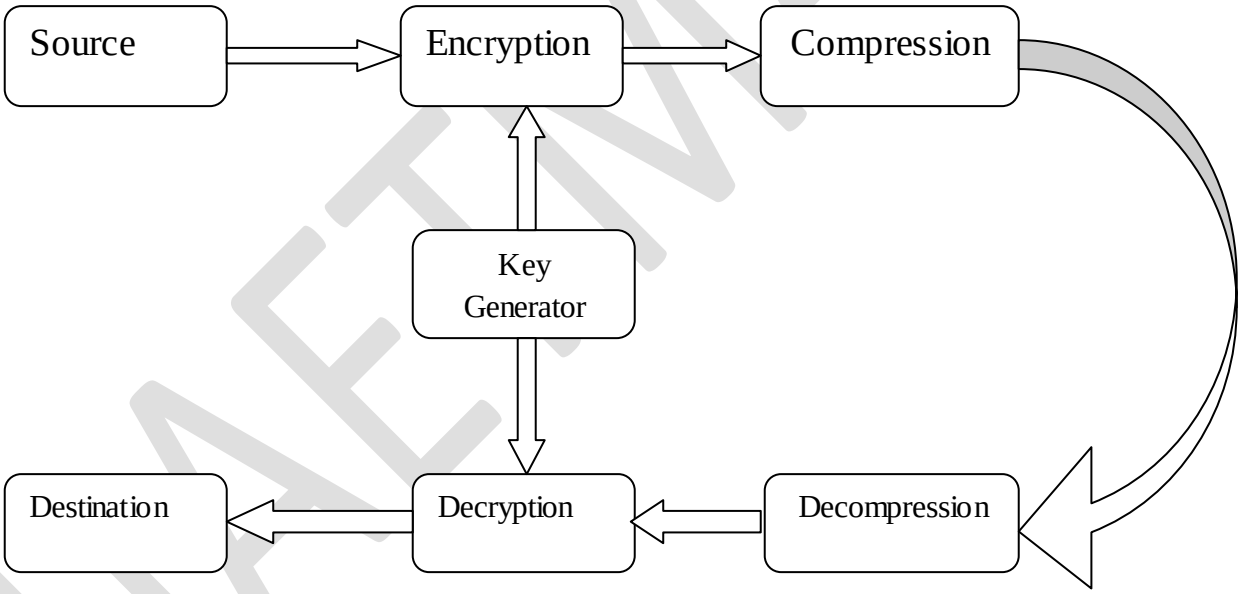

Fig.1 Block diagram of the proposed method

Fig. 1 represents the overall operations involved in the proposed system. At the source, image to be transmitted is encrypted first. It is followed by compression process. Compressed image will be sent to the destination. At the destination, received image will be decompressed first. Next, this decompressed image undergoes decryption process which gives original image as the output. Since the proposed method is based on symmetric key encryption, same key is used for both encryption and decryption.

International Journal of Advancement in Engineering Technology, Management & Applied Science
Volume 3, Issue 6 June 2016 ISSN No: 2349-3224

1. Encryption

Secret key plays a major role in encryption. Five Feedback Shift Register (FSR) of length 19, 22, 23, 16, and 16 respectively have been used for generating the 10 bits length secret key. This process is shown in the fig. 2. First the pixels of the input image will be extracted. One pixel will be taken at a time, on which sieving process will be applied. Extracted red, green, and blue components will be encrypted twice, individually.

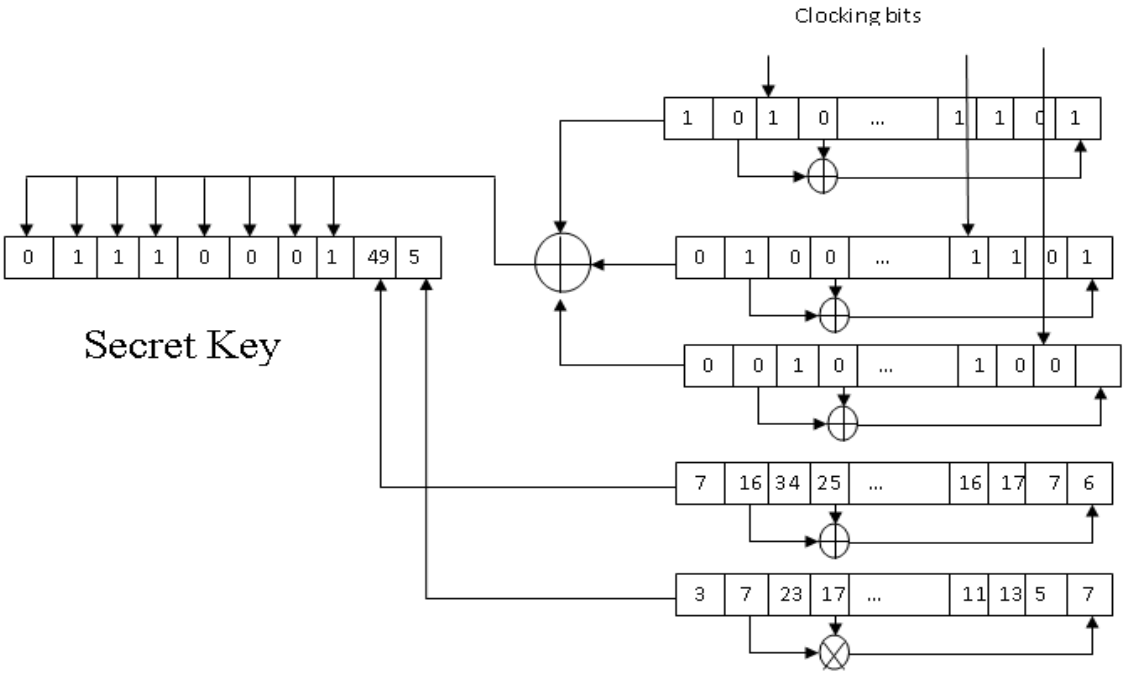

Fig. 2 Process of Secret Key Generation

As shown in the figure 2, five FSRs have been used to generate the secret key. First three FSRs contains only binary numbers as the seed values, fourth and fifth FSRs takes integer values as the seed values. In each of the first three FSRs, one bit is taken as a clocking bit. It indicates whether the respective FSR has to be shifted or not. After each interval, majority of the clocking bits is computed. The FSR with majority bit as its clocking bit will be left shifted by one position. Criteria for Shifting is shown in the Table I

1.1) Modular additive encryption:

In this type of encryption, first 9 bits of the secret key will be used to encrypt the three color components of the pixel.

General Syntax is as follows:

Enc. Red1 = (red + secret key1) mod 256

Enc. Green1 = (green + secret key1) mod 256

Enc. Blue1 = (blue + secret key1) mod 256

where secret key1 is the sum of decimal conversion of the first eight bits of the key and the ninth bit value.

TABLE I

CRITERIA FOR SHIFTING THE FEEDBACK SHIFT REGISTERS

	FSR1	**FSR2**	**FSR3**	**Majority Bit**	**Shift**
Clocking Bit Value	0	0	0	0	ALL
	0	0	1	0	FSR1, FSR2
	0	1	0	0	FSR1,FSR3
	0	1	1	1	FSR2, FSR3
	1	0	0	0	FSR2,FSR3
	1	0	1	1	FSR1, FSR3
	1	1	0	1	FSR1, FSR2
	1	1	1	1	ALL

1.2) Modular Multiplicative Encryption:

Here, last bit of the secret key will be modularly multiplied with the encrypted red, green, and blue colors. This two time encryption ensures more security.

General syntax is,

Enc. Red2 = (enc. Red1 * secret key2) mod 256

Enc. Green2 = (enc. Green1 * secret key2) mod 256

Enc. Blue2 = (enc. Blue1 * secret key2) mod 256

After encryption, three color components will be merged together which in turn forms encrypted pixel.

2. Compression

Deflater class of java has been used to achieve compression. It takes the byte values of the encrypted pixels as the input and produces compressed array of bytes.

3. Decompression

Decompression has been done using inflater class of java. It takes the compressed array of bytes as the input and produces the bytes array which is of original size.

4. Decryption

Decryption is the reverse process of the encryption. First, from the encrypted pixels, red, green, and blue components will be extracted. Since modular additive encryption is followed by the modular multiplicative encryption in case of encryption, here, inverse of the modular multiplicative encryption will take place first.

4.1) Inverse modular multiplicative encryption:

Here, inverse of the secret key used for encryption will be multiplied with the encrypted color values. General syntax is as follows:

Dec. red1 = (enc. Red * inverse(secret key1))mod 256

Dec. green1 = (enc. green * inverse(secret key1)) mod 256

Dec. blue1 = (enc. blue * inverse(secret key1)) mod 256

Where secret key1 is the last bit value of the 10 bit secret key.

Inverse of the secret key can be calculated using the following syntax:

Inverse of key = ((key * x) mod 256)= 1

Where x is a number which is relative prime of 256.

4.2) Inverse modular additive encryption:

In this type of decryption, first 9 bits of the secret key will be used to decrypt the three color components of the pixel.

General Syntax is as follows:

Dec. Red2 = (dec red1 - secret key1) mod 256
Dec. Green2 = (dec green1 - secret key1) mod 256
Dec. Blue2 = (dec blue1 - secret key1) mod 256

where secret key2 is the sum of decimal conversion of the first eight bits of the key and the ninth bit value.

These decrypted color components will be combined together to form the original pixels.

1V. PERFORMANCE AND SECURITY ANALYSIS

Fig. 3 shows the input image. Fig. 4 shows the encrypted image created by the proposed method. From this figure, it is clear that, original image has been encrypted properly, that is without any trace by the proposed method. Also, it can be observed that , even if a third party captures the image, he can't predict the encrypted contents just by looking at the image.

IJAETMAS

Fig. 3 Input image

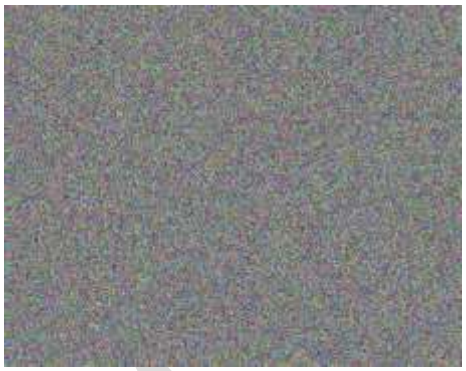

Fig. 4 Encrypted Image

Fig.5 Decrypted Image

Fig. 5 shows the decrypted image. From the comparison between the original image, and the decrypted image, it is clear that, encrypted image has been decrypted successfully by the proposed method.

1. Histogram Analysis

Image histogram is a very important feature in image analysis. It specifies the number of occurrence of each pixel in the image. From the figure 7 it is observed that the histogram of the encrypted image for red part of the pixel is nearly uniform and meaningfully different from the histograms of the original image for the respective color shown in the fig. 6. Hence it does not provide any clue to employ any statistical analysis attack on the encryption image.

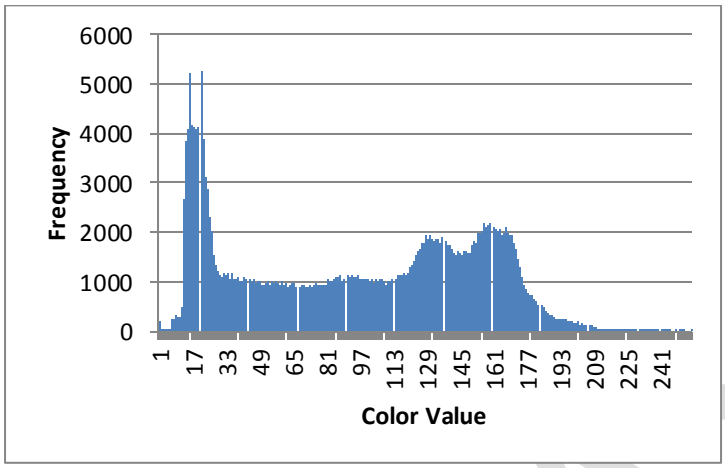

Fig. 6 Histogram of the red pixel for the original image

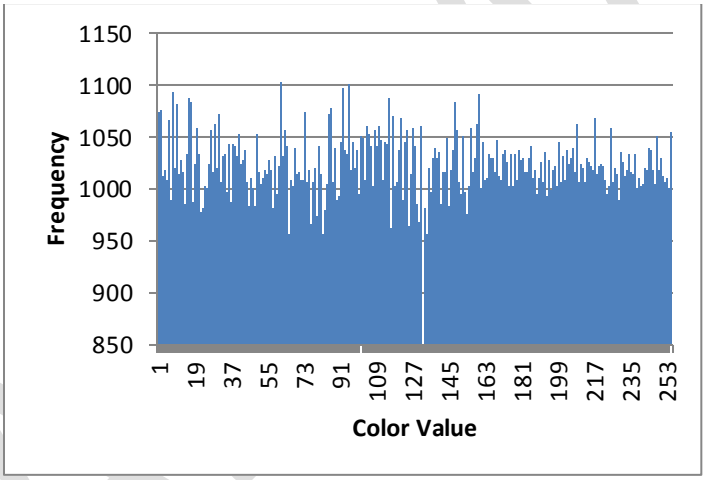

Fig. 7 Histogram of the red pixel for the encrypted image

2. Avalanche Effect

Avalanche effect indicates that, one bit change in the key or in the original pixel value, should results in a large change in the encrypted image. In figure 4.6, blue line indicates the original pixel values for color red from the range 1000 to 1025. Brown line indicates the encrypted red pixel values for the seed values 3, 7, 11, 23, 13, 17, 67, 23, 11, 5, 7, 3, 37, 43, 3, 7. Green line represents the encrypted pixel values for one bit change in the key. That is, last seed value "7" has been changed to "3" for this encryption. From the two sets of encrypted values it is clear that, even if

someone uses bruteforce method to decrypt the image, it will be very difficult to find the original values because of the large variation of the values.

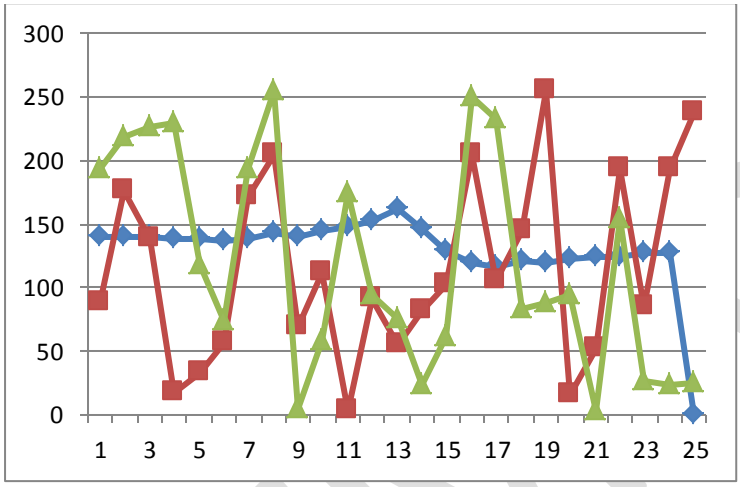

Fig. 8 Avalanche effect of red pixel value of the image for the pixels between 1000 and 1025 for proposed method

V. COMPARISON WITH THE EXISTING METHODS

In the following subsections security parameters such as Standard deviation, entropy, and quality of encryption of the proposed method are compared with the respective parameters of the existing methods listed in the table 4.1. All the methods have been implemented by using NetBeans IDE.

Serial No.	Method Name
1	Modular multiplicative encryption using single FSR
2	Modular multiplicative encryption using double FSR
3	Modular multiplicative encryption using triple FSR
4	Transposition cipher
5	Transposition cipher with modular multiplicative encryption

Table II: EXISTING ENCRYPTION METHODS

1. Standard Deviation Comparison

A less standard deviation means that the colors are distributed uniformly. Following equation can be used to calculate the standard deviation.

$$\text{Standard Deviation, } \sigma = \sqrt{\frac{1}{N}\sum_{i=0}^{N}(y_i - \mu)^2}$$

$$\text{Mean, } \mu = \frac{\sum_{i=1}^{N} Y_i}{N}$$

Where,

N = Total number of pixels

y_i = Frequency of occurrence of each pixel value

μ = Mean value

TABLE III
COMPARISON OF THE STANDARD DEVIATION OF THE PROPOSED METHOD WITH THE EXISTING METHODS LISTED IN THE TABLE II

Methods	Standard Deviation		
	Red	Green	Blue
Original	935.5338	960.6659	1470.276
Method1	113.5434	143.2755	174.6914
Method2	111.2679	138.9699	161.6706
Method3	100.6868	128.1821	147.0388
Method4	935.5338	960.6659	1470.276
Method5	116.7789	143.3254	174.5185
Proposed Method	27.46834	26.9942	28.21542

From the Table III, it is clear that standard deviation of the proposed method is better than the existing methods listed in the Table II. Standard deviation for the proposed method is very less compared to that for the original image. It indicates that the pixels are distributed almost uniformly in the encrypted image. It helps in sustaining against the frequency attack.

2. Entropy Comparison

Entropy helps in neutralizing the amount of information present in the plaintext. So an attacker cannot use this information to decrypt the data. As it can be observed from the below table, that the entropy of the proposed method for red, green, and blue components are higher than the entropy of the other methods for the respective colors. So it can be concluded that, proposed method is capable to prevent the security attacks.

TABLE IV

COMPARISON OF THE ENTROPY OF THE PROPOSED METHOD WITH THE EXISTING METHODS LISTED IN THE TABLE II

Methods	Entropy		
	Red	Green	Blue
Original	7.392943	7.392251	7.057988
Method1	7.990641	7.986597	7.980289
Method2	7.991001	7.987305	7.983065
Method3	7.992493	7.98893	7.985667
Method4	7.392943	7.392251	7.057988
Method5	7.990156	7.98629	7.979928
Proposed Method	7.999484	7.999503	7.999456

3. Quality of Encryption(QoE) Comparison

Quality of Encryption is the sum of the absolute difference between the original pixel value and the encrypted pixel value. A good encryption system exhibits a high QoE value.

TABLE V

COMPARISON OF THE ENTROPY OF THE PROPOSED METHOD WITH THE EXISTING METHODS LISTED IN THE TABLE II

Methods	Quality of Encryption		
	Red	Green	Blue
Method1	81	81	74
Method2	81	81	74
Method3	83	82	74
Method4	64	63	51
Method5	80	80	74
Proposed Method	88	86	85

As it can be observed from the above table, QoE of the proposed method is better than the existing methods. So it can be said that, proposed method has the ability to tolerate the security attacks.

VI. CONCLUSION

In this paper it has been provided the method for improving the image security along with this size of the image to be transmitted also be reduced First, encryption has been done using ten bits secret key. It is followed by the compression of the encrypted image. The evaluation parameter such as quality of encryption, standard deviation , entropy and avalanche effect also shows the strength of the encryption. It has been observed in this , since it is a stream cipher the same key has been used for both encryption and decryption. From the results obtained, and the comparisons of standard deviation, entropy, avalanche effect, histogram analysis, and quality of encryption of the proposed method with the respective parameters of the existing methods, it is clear that, proposed method has the potential to sustain the security attacks. Also due to the compression the data to be transmitted is again reduced.

REFERENCES

[1] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani" A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013), pp.275-290

[2] Quist-Aphetsi Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015

[3] Komal D Patel,"Image Encryption Using Different Techniques:A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 1, pp. 30-34, Nov 2011.

[4] Abdul Razzaque and Dr. Nileshsingh V.Thakur "An Approach to Image Compression with Partial Encryption without sharing the Secret Key", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012

[5] Alavi Kunhu and Hussain Ahmad, "Multi Watermarking Algorithm Based on DCT and Hash Functions for Color Satellite Images" , IEEE 2013

[6] M.Sithi Benazir, Dr.A.Padmapriya, "Elementary Matrix Operation Based Satellite Image Encryption", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[7] Ravi Prakash Dewangan, Chandrashekhar Kamargaonkar, "Compression of Encrypted Image using Wavelet Transform", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04

[8] Rajinder Kaur, Er.Kanwalprit Singh, "Image Encryption Techniques:A Selected Review",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278- 0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83

[9] Pankesh Bamotra "Image Encryption Using Pixel Shuffling", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper

[10] Bhagwati Prasad, Kunti Mishra "A Combined Encryption Compression Scheme Using Chaotic Maps", Cybernetics and information technologies , Volume 13, No 2, 2013

IJAETMAS